Related-Key Boomerang Attack on Block Cipher SQUARE

Bonwook Koo[1,2], Yongjin Yeom[1], and Junghwan Song[2]

[1] The Attached Institute of ETRI
P.O.Box 1, Yuseong-Gu, Deajeon, Korea
{bwkoo,yjyeom}@ensec.re.kr
[2] CAMP Lab., Hanyang University
17 Haengdang-dong, Seongdong-gu, Seoul, 133-791, Korea
camp123@hanyang.ac.kr

Abstract. SQUARE is 8-round SPN structure block cipher and its round function and key schedule have been slightly modified to design building blocks of Rijndael. Key schedule of SQUARE is simple and efficient but fully affine, so we apply a related-key attack on it.
We find a 3-round related-key differential trail with probability 2^{-28}, which have zero differences both on its input and output states, and this trail is called the *local collision* in [5]. By extending of this related-key differential, we construct a 7-round related-key boomerang distinguisher and successful attack on full round SQUARE. The best attack on SQUARE have ever been known is the *square attack* on 6-round reduced variant of SQUARE.
In this paper, we present a key recovery attack on the full round of SQUARE using a related-key boomerang distinguisher. We construct a 7-round related-key boomerang distinguisher with probability 2^{-119} by finding *local collision*, and calculate its probability using *ladder switch* and *local amplification* techniques. As a result, one round on top of distinguisher is added to construct a full round attack on SQUARE which recovers 16-bit key information with 2^{36} encryptions and 2^{123} data.

Key words: SQUARE, Related-key boomerang attack, block cipher, AES

1 Introduction

The block cipher SQUARE [8] was designed by Joan Daemen, Lars Knudsen, and Vincent Rijmen and two of them are the designers of Advanced Encryption Standard (AES) [11]. Since the structure and mathematical logics that used in both block ciphers SQUARE and AES are similar, so SQUARE is considered as a predecessor of AES.

Attacks on AES-192 and AES-256 [4–6] have been discussed and those attacks are based on the related-key model [1]. In [5], Biryukov, et al. have shown successful attacks on the full round AES-192 and AES-256 using a related-key boomerang distinguisher, where some helpful techniques have been added such as *local collision*, Feistel switch, *ladder switch*, and so on.

In this paper, we construct a related-key boomerang distinguisher with *local collision* and *ladder switch* techniques to attack the block cipher SQUARE. In addition, a simple idea *local amplification* is used to calculate a lower bound to be increased in the value of the distinguisher's probability.

Local amplification is based on the fact that the coincidence of differences at the switching point of both lower trail is enough to construct a related-key boomerang distinguisher, thus we gather these probabilities of trails so that a factor of distinguisher's probability is amplified from 2^{-14} to 2^{-7}. Therefore, we get a better estimation for probability of distinguisher which is greater than 2^{-128}.

1.1 Related works

SQUARE is designed under the *Wide Trail Strategy* to guarantee security against differential and linear cryptanalysis and the designers of SQUARE have claimed that 6-round SQUARE is sufficiently secure against differential and linear cryptanalysis. Also they have given a dedicated attack which is called *Square Attack*, and by this attack, at most 6-round SQUARE would be attacked with 2^{72} complexity. There are no more attack results on the block cipher SQUARE so far.

In 2005, the related-key boomernag attack has been applied to several ciphers KASUMI [3], COCONUT98 [2], IDEA [2], and AES-192/256 [5]. In [3], authors have given a related key boomerang attack on KASUMI reduced to 6-round out of 8-round with 34 related-keys and 2^{13} time complexity, and also they have shown that the full round KASUMI could be attacked with 4 related-keys and $2^{78.7}$ time complexity by transforming boomerang attack into chosen ciphertext/adaptive chosen plaintext attack. Full round COCONUT98 was easily distinguished by 1 related-key boomerang quartet with 2 related keys in [2] and the authors presented key recovery attack on 6-round IDEA out of 8.5-round using related-key boomerang distinguisher with 4 related-key and $2^{51.6}$ data complexity.

In 2008, Gorski et al. presented the first related-key boomerang attacks on reduced round of AES-192 [9]. They gave an attack on 7-round AES-192 with only 2^{18} chosen plaintext and $2^{67.5}$ encryptions and extend it to the attack on 9-round AES-192 with 2^{67} chosen plaintext and $2^{143.33}$ encryptions.

At last, in 2009, related-key boomerang attacks on full round AES-192 and AES-256 are presented at ASIACRYPT2009 by Biryukov et, al [5]. They uses differential trails including *local collision* and some boomerang switching techniques such as *ladder switch*, *Feistel switch*, and *s-box switch*. Their attack on AES-192 requires 2^{176} encryptions and 2^{123} data and on AES-256 requires 2^{119} encryptions and data.

2 Description of block cipher SQUARE

The size of block, master key, and round keys of SQUARE are all 128-bit. The followings are the different representations of a 128-bit data $X \in \underbrace{\mathrm{GF}(2^8) \times \cdots \times \mathrm{GF}(2^8)}_{16\text{times}} =$

$\mathrm{GF}(2^8)^{16}$.

$$X = (x_0, x_1, ..., x_{15}) = \begin{array}{|c|c|c|c|}\hline x_0 & x_1 & x_2 & x_3 \\ \hline x_4 & x_5 & x_6 & x_7 \\ \hline x_8 & x_9 & x_{10} & x_{11} \\ \hline x_{12} & x_{13} & x_{14} & x_{15} \\ \hline \end{array} = \begin{array}{|c|c|c|c|}\hline x_{0,0} & x_{0,1} & x_{0,2} & x_{0,3} \\ \hline x_{1,0} & x_{1,1} & x_{1,2} & x_{1,3} \\ \hline x_{2,0} & x_{2,1} & x_{2,2} & x_{2,3} \\ \hline x_{3,0} & x_{3,1} & x_{3,2} & x_{3,3} \\ \hline \end{array},$$

where x_i and $x_{j,k} \in \mathrm{GF}(2^8)$.

Let an irreducible polynomial p be $p(x) = x^8 + x^4 + x^3 + x + 1$ over GF(2), which is the same one to define the finite field $\mathrm{GF}(2^8) = \mathrm{GF}(2)[x]/\langle p(x)\rangle$ as in AES.

SQUARE is an 8-round SPN block cipher with 9 round keys. The round transformation ρ, which is a composition of four functions such as θ, γ, π, and σ, is as the following.

$$\rho_{rk^i}(X) = \sigma_{rk^i} \circ \pi \circ \gamma \circ \theta(X).$$

The θ consists of 4 times of row-wise matrix multiplications over $\mathrm{GF}(2^8)$. The following 4×4 MDS matrix $\mathcal{M}$ represent the function θ and is the same matrix of `MixColumns` in AES.

$$\mathcal{M} = \begin{pmatrix} \mathtt{02\ 03\ 01\ 01} \\ \mathtt{01\ 02\ 03\ 01} \\ \mathtt{01\ 01\ 02\ 03} \\ \mathtt{03\ 01\ 01\ 02} \end{pmatrix}.$$

The γ is a byte-wise S-box operation with identical S-boxes. Since no specific S-box is given in [8], we choose an S-box which is the same as to AES. The choice of S-box can affect the complexity of our attack. However, every S-box defined by an affine transformation of inversion over a finite field $\mathrm{GF}(2^8)$ have the same aspect against our attack, and this kind of S-box is the most wide used one. Therefore, our assumption does not lose generality. The π is a transposition of 4×4 data array and the σ is a round key addition.

The key schedule of SQUARE is quite similar to the key schedule of AES-128. Adding S-boxes and transposition of round keys are the only modification to the key schedule of AES-128. Figure 1 shows structure of key schedule of SQUARE.

Let $rk^0, rk^1, \cdots, rk^8$ be nine 128-bit round keys the first round key rk^0 be the master key K. Each i-th round key $rk^i (i = 0, 1, \cdots, 8)$ is regarded as a 4×4 byte array and let rk^i_j represent the j-th row of i-th round key. The round key generation function ψ generates each row of the $(i+1)$-th round key from the i-th round key as follows.

$$\begin{aligned} rk_0^{i+1} &= rk_0^i \oplus \mathsf{rotl}(rk_3^i) \oplus C^i, \\ rk_1^{i+1} &= rk_1^i \oplus rk_0^{i+1}, \\ rk_2^{i+1} &= rk_2^i \oplus rk_1^{i+1}, \\ rk_3^{i+1} &= rk_3^i \oplus rk_2^{i+1}. \end{aligned}$$

The byte rotation function, $\mathsf{rotl} : \mathrm{GF}(2^8)^4 \to \mathrm{GF}(2^8)^4$ is defined by

$$\mathsf{rotl}[a_0, a_1, a_2, a_3] = [a_1, a_2, a_3, a_0],$$

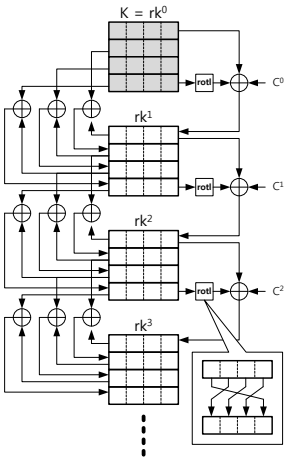

Fig. 1. Key schedule of SQUARE

and each C^i is a constant generated from the previous constant C^{i-1} by the relation $C^i = 2 \times C^{i-1}$, where $C^0 = 1$ over GF(2^8). Therefore, the block cipher SQUARE is represented by the following composition of functions.

$$\text{SQUARE}_K(X) = \rho_{rk^8} \circ \rho_{rk^7} \circ \rho_{rk^6} \circ \rho_{rk^5} \circ \rho_{rk^4} \circ \rho_{rk^3} \circ \rho_{rk^2} \circ \rho_{rk^1} \circ \sigma_{rk^0} \circ \theta^{-1}(X).$$

3 Local Collision of SQUARE

The idea of local collision property is firstly used for cryptanalysis of hash functions [7] and it has been used to attack block ciphers in the related-key attack model [5].

We find a family of related-key differentials of block cipher SQUARE in which a local collision occurs as described in Figure 2. Let a symbol ▣ represent an

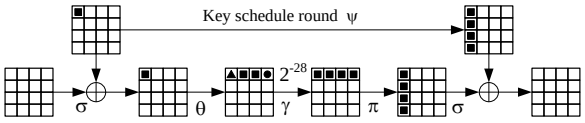

Fig. 2. A local collision in SQUARE

one byte difference value, then symbols ▲ and ◉ denote the values 2· ▣ and 3· ▣ over GF(2^8), which are defined by the linear function θ, respectively. Note that the blank box implies one byte difference whose value is 0.

By a differential property of the S-box, there are 22 out of 255 possible nonzero differences ▣ , which satisfy the related-key differential depicted in Figure 2. The following set is the collection of all 22 possible differences in hexadecimal forms.

$$\mathcal{A} = \{\texttt{0a}, \texttt{11}, \texttt{17}, \texttt{1d}, \texttt{20}, \texttt{3b}, \texttt{4d}, \texttt{53}, \texttt{73}, \texttt{76}, \texttt{7c}, \texttt{87}, \texttt{9d}, \texttt{a4}, \texttt{a8}, \texttt{ae}, \texttt{c6}, \texttt{d2}, \texttt{d5}, \texttt{e0}, \texttt{ee}, \texttt{fc}\}.$$

Throughout this paper, we let ▣ denote one byte difference value `0x0a`, because each probability of differential in Figure 2, where each element in the set $\mathcal{A}$ regarded as ▣, is all equal to 2^{-28}. Note that symbols ▲ and ◉ are calculated as `0x14` and `0x1e` by the matrix $\mathcal{M}$, respectively.

Let $\mathcal{C}_i$ be a composition of σ function of i-th round and three following round functions such as

$$\mathcal{C}_i = \rho_{rk^{i+3}} \circ \rho_{rk^{i+2}} \circ \rho_{rk^{i+1}} \circ \sigma_{rk^i}.$$

Then we can construct a trail of 3-round related-key differential denoted by $\mathcal{C}_i$ as described in Figure 3.

In Figure 3, an input difference of $\mathcal{C}_i$ is canceled by i-th round key difference Δrk^i so that the input difference of the next round function $\rho_{rk^{i+2}}$ becomes to equal to Δrk^{i+1}.

During the procedure that Δrk^{i+1} is transformed into Δrk^{i+2} with probability 1 by the function ψ, Δrk^{i+1} is transformed into Δrk^{i+2} with probability 2^{-28} via the other way induced from the functions θ, γ, and π.

Therefore, the probability of the related-key differential trail of $\mathcal{C}_i$ is 2^{-28}, and it is easy to check that the probability of the the same trail in reverse direction is also 2^{-28}.

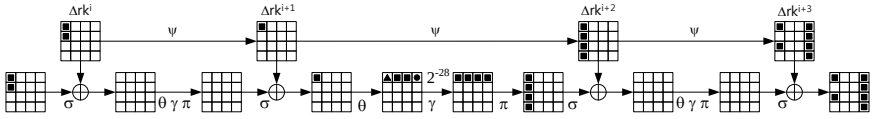

Fig. 3. A 3-round related-key differential trail for $\mathcal{C}_i$

Using the related-key differential trail described above, we construct a 7-round related-key distinguisher with probability greater than 2^{-128}.

4 Related-key Boomerang Attack

In this section, related-key boomerang attack is explained in briefly together with additional techniques, such as *local amplification* and *ladder switch*.

4.1 Boomerang Distinguisher and Related-Key Attack Model

A block cipher $E_K : \{0,1\}^n \to \{0,1\}^n$ with an arbitrary key K can be represented by a composition of two sub-ciphers $E0_K$ and $E1_K$, where $E_K = E1_K \circ E0_K$. If there exist both differentials $(\Delta P \to \Delta Y)$ for $E0_K$ and $(\Delta Y \to \Delta P)$ for $E0_K^{-1}$ with probability p, and a differential $(\nabla C \to \nabla Y)$ for $E1_K^{-1}$ with probability q. Then, for a chosen plaintext pair (P_1, P_2) such that $P_1 \oplus P_2 = \Delta P$, the corresponding plaintext pair (Q_1, Q_2) calculated by

$$Q_1 = E_K^{-1}(E_K(P_1) \oplus \nabla C),$$
$$Q_2 = E_K^{-1}(E_K(P_2) \oplus \nabla C),$$

satisfies $Q_1 \oplus Q_2 = \Delta P$ with the boomerang probability p^2q^2.

In the related-key attack model, attackers need to know or choose relations between several keys. The relation between keys for this attack is simply difference. Since the structure of the key schedule of SQUARE is fully linear or affine, each operation for key schedule preserves difference properties. So, no matter what a key differential trail is assumed to be used, its probability is always 1.

The related-key boomerang attack uses 2 or more related-keys, and we consider 4 related-keys $K1$, $K2$, $K3$, and $K4$ for our attack which have the following relations,

$$\Delta K = K1 \oplus K2 = K3 \oplus K4,$$
$$\nabla K = K1 \oplus K3 = K2 \oplus K4.$$

The related-key boomerang distinguisher with above related-keys is described as follows. Assume that both the probabilities of related-key differential $(\Delta P \to \Delta Y)$ for $E0_{\Delta K}$ and of $(\Delta Y \to \Delta P)$ for $E0_{\Delta K}^{-1}$ are p, and the probability of a related-key differential $(\nabla C \to \nabla Y)$ for $E1_{\nabla K}^{-1}$ is q, where the notation $E_{\Delta K}$ implies a pair of encryption E with related-key pair whose difference is ΔK. Then, for a chosen plaintext pair (P_1, P_2) such that $P_1 \oplus P_2 = \Delta P$, the corresponding plaintext pair (Q_1, Q_2) calculated by

$$Q_1 = E_{K3}^{-1}(E_{K1}(P_1) \oplus \nabla C),$$
$$Q_2 = E_{K4}^{-1}(E_{K2}(P_2) \oplus \nabla C),$$

satisfies $Q_1 \oplus Q_2 = \Delta P$ with the boomerang probability p^2q^2. Boomerang distinguisher is a special case of related-key boomerang distinguisher with $\Delta K = \nabla K = 0$.

4.2 Additional Techniques

A boomerang distinguisher enables us to estimate the lower bound of probability that we successfully observe the distinguishing property. We can estimate the lower bound more precisely by using the following techniques.

Local Amplification. In $E1$, contrary to plain boomerang distinguisher, both output differences $E1_{K1}^{-1}(C_1) \oplus E1_{K3}^{-1}(C_1 \oplus \nabla C)$ and $E1_{K2}^{-1}(C_2) \oplus E1_{K4}^{-1}(C_2 \oplus \nabla C)$ do not need to be equal to a value ∇Y, it is enough that they are equal to each other to satisfy the following equation,

$$E1_{K3}^{-1}(C_1 \oplus \nabla C) \oplus E1_{K4}^{-1}(C_2 \oplus \nabla C) = \Delta Y. \tag{1}$$

Suppose that $E1$ is a composition of two sub-functions e_0 and e_1 such that $E1 = e_1 \circ e_0$ and there exists a related-key differential trail $(\nabla C \rightarrow \nabla D \rightarrow \nabla Y)$ for $E1_{\nabla K}^{-1}$ with probability q. Let $\tilde{q}$ denote the probability of differential $(\nabla C \rightarrow \nabla D)$ for e_1^{-1} and let r denote the probability of differential $(\nabla D \rightarrow \nabla Y)$ for e_0^{-1}. Then the probability of differential trail $(\nabla C \rightarrow \nabla D \rightarrow \nabla Y)$ is bounded below by $q = \tilde{q} \times r$.

If there exist other $\nabla Y_0, \nabla Y_1, \cdots, \nabla Y_{n-1}$ with corresponding nonzero probabilities $r_i (i = 0, 1, \cdots, n-1)$ of differentials $(\nabla D \rightarrow \nabla Y_i)(i = 0, 1, \cdots, n-1)$ for e_0^{-1}, then we can denote each probability of differential trail $(\nabla C \rightarrow \nabla D \rightarrow \nabla Y_i)$ by $q_i = \tilde{q} \times r_i$ for $i = 0, 1, \cdots, n-1$. So the probability that the equation (1) holds is estimated by the sum of all q_i^2 for $i = 0, 1, \cdots, n-1$ and we denote this probability by

$$\hat{q}^2 = \sum_{i=0}^{n-1} q_i^2 = \tilde{q}^2 \times \sum_{i=0}^{n-1} r_i^2.$$

Therefore, we have the following probability of locally amplified boomerang distinguisher,

$$p^2 \hat{q}^2 = p^2 \times \tilde{q}^2 \times \sum_{i=0}^{n-1} r_i^2. \tag{2}$$

Ladder Switch. Briyukov et. al have proposed a technique in [5] which minimizes the number of active S-boxes in a boomerang distinguisher.

They use the parallelism of S-box operations so that some of S-boxes can be regarded as parts of $E0$ and the others as parts of $E1$.

If there exist an S-box which is active when it is regraded as a part of $E1$, but not a part of $E0$, then we define $E0$ by the previous functions of the substitution layer and the target S-box. And also we define $E1$ by the rest of S-boxes other than the target S-box and functions after the substitution layer. Then the probability of the boomerang distinguisher is independent with the target S-box.

5 The Trails and Related-Key Boomerang Distinguisher

5.1 Related-key differential trails for $E0$ and $E1$

A related-key boomerang distinguisher of our attack consists of two similar related-key differential trails $E0$ and $E1$ depicted in Figure 4 and Figure 5. $E0$ and $E1$ are divided so as to apply the *ladder switch* technique as follows. Let $S_{i,j}$ be the i-th S-box of the j-th column, where γ is considered as a 4×4 array

of S-boxes. In γ of 5-th round, only one S-box $S_{0,1}$ is included in $E0$ and others are included $E1$, because in the related-key differentials of $E0$ and $E1$ that we use, $S_{0,1}$ of 5-th round is active in $E1$ but not active in $E0$. So we do not pay probability 2^{-7} for $S_{0,1}$ of 5-th round by including the S-box in $E0$.

We define $E0$ by $S_{0,1} \circ \theta \circ \mathcal{C}_1$ and we know that the probability of related-key differential $\mathcal{C}_1$ is 2^{-28}. The first row $(\texttt{0x0a}, \texttt{0x00}, \texttt{0x00}, \texttt{0x0a})$ of output difference of $\mathcal{C}_1$ is transformed into $(\texttt{0x1e}, \texttt{0x00}, \texttt{0x14}, \texttt{0x0a})$ by the matrix $\mathcal{M}$ thus $S_{0,1}$ of the last round in $E0$ is not an active S-box. Therefore, the probability of related-key differential trail of $E0$ is still 2^{-28}(see Figure 4), and the probability p in equation (2) is 2^{-28}. Note that the symbols ⊠ indicate 8-bit difference values which is not critical for this attack.

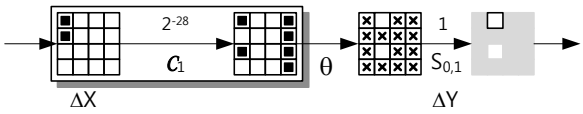

Fig. 4. related-key differential trail of $E0$

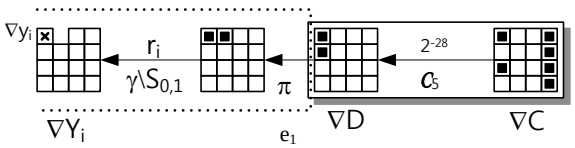

Fig. 5. related-key differential trail of $E1$

Let $E1 = \mathcal{C}_5 \circ \pi \circ (\gamma \setminus S_{0,1})$, and $e_0 = \pi \circ (\gamma \setminus S_{0,1})$. Then, we consider $E1$ as a composition of two sub-functions e_0 and $\mathcal{C}_5$ so we apply the local amplification to calculate the differential probability of $E1$. Differential trail of $E1$ proceeds in reverse direction(see Figure 5). The probability of related-key differential trail for $\mathcal{C}_5^{-1}$ is 2^{-28}, and we let $\tilde{q}$ be 2^{-28}. We let $\nabla y_i (i = 0, 1, \cdots, 255)$ be the values of each byte difference for ⊠. Since there is only one active S-box $S_{0,0}^{-1}$ in e_1^{-1}, the probability of differential trail for e_0^{-1} equals to the differential probability of $S_{0,0}^{-1}$. The probabilities of differential $(\texttt{0x0a} \rightarrow \nabla y_i)$ by $S_{0,0}^{-1}$ are 0 for 128 values of y_i, 2^{-7} for 126 values of ∇y_i, and 2^{-6} for 1 value of ∇y_i. If we let the probability of related-key differential $(\texttt{0x0a} \rightarrow \nabla y_i)$ by r_i for each ∇y_i then probability of related-key differential trail from ∇C to ∇Y_i by $E1_{\nabla K}^{-1}$ is

$$q_i = 2^{-28} \times r_i.$$

5.2 7-Round related-key Boomerang Distinguisher

As discussed above, $p = 2^{-28}$ and $q_i = 2^{-28} \times r_i$ for each ∇Y_i. The probability which a pair (X_1, X_2) with difference ΔX is transformed into the output pair (X_3, X_4) whose difference is ΔX, through the related-key boomerang distinguisher depicted in Figure 6 is

$$p^2\hat{q}^2 = p^2 \times \tilde{q}^2 \times \sum_{i=0}^{n-1} r_i^2 = 2^{-28\times 2} \times 2^{-28\times 2} \times \sum_{i=0}^{n-1} r_i^2 = 2^{-112} \times \sum_{i=0}^{n-1} r_i^2.$$

There are 127 values for ∇Y_i which have nonzero probabilities r_i and among these ∇Y_i, 126 values have the probability 2^{-7} and one value has the probability 2^{-6}. Therefore, the related-key boomerang quartet (X_1, X_2, X_3, X_4) which satisfies all trails of distinguisher, occurs with the probability

$$p^2\hat{q}^2 = 2^{-112} \times \sum_{i=0}^{126} r_i^2 = 2^{-112} \times (2^{-12} + 126 \times 2^{-14}) \geq 2^{-119},$$

and we call this quartet as right quartet.

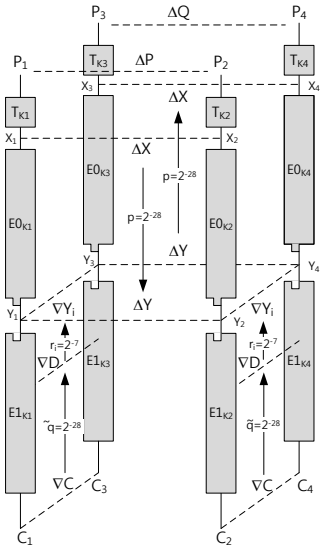

Fig. 6. A 7-round related-key boomerang distinguisher and additional round T

T_K in the Figure 6 is going to be discussed in the following section.

5.3 Additional Round T

As depicted in Figure 6, an additional round T, before $E0$ is need to make $E1 \circ E0 \circ T$ to be full round SQUARE. Let us define T as follows.

$$T = \pi \circ \gamma \circ \theta \circ \sigma_{rk^0} \circ \theta^{-1}.$$

By the linearity of θ, σ, and ψ, T can be represented by

$$T = \pi \circ \gamma \circ \sigma_{\theta(rk^0)}.$$

For this attack, related-key differential trail of the additional round T in Figure 7 is used. T contains S-box layer γ which has 2 active S-boxes in it, so the probability of this differential trail is strictly smaller than 1. However, we can construct a structure(set of pairs) such that a fixed portion of plaintext pairs always satisfy the trail. In T, if we consider a set of plaintext pairs with differences ΔP, where ΔP is an arbitrary element of the set $\mathcal{P}$ defined by

$$\mathcal{P} = \{(\alpha, \beta, \texttt{0a}, \texttt{1e}, \quad \texttt{00}, \texttt{00}, \texttt{00}, \texttt{00}, \quad \texttt{14}, \texttt{0a}, \texttt{0a}, \texttt{1e}, \quad \texttt{00}, \texttt{00}, \texttt{00}, \texttt{00}) | \alpha, \beta \in \mathrm{GF}(2^8)\}. \tag{3}$$

Then, output differences of all pairs must be ΔX with ratio 2^{-16}.

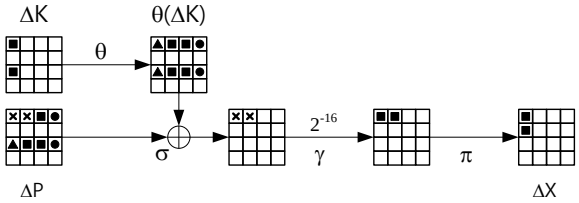

Fig. 7. related-key differential trail of additional round T

5.4 Differential trails of round keys

As we pointed out above, the round function ψ of key schedule of SQUARE preserves XOR operation, so a master key difference generates only one key differential trail with probability 1. Two key differential trails derived from master key differences ΔK and ∇K for our attack are depicted in Figure 8. Note that the gray parts of the key differential trails are not used for this attack. The trail derived from ΔK is for sub-cipher $E0$ and from ∇K is for $E1$, and these key differential trails occur local collisions both in $E0_{\Delta K}$ and $E1_{\nabla K}$.

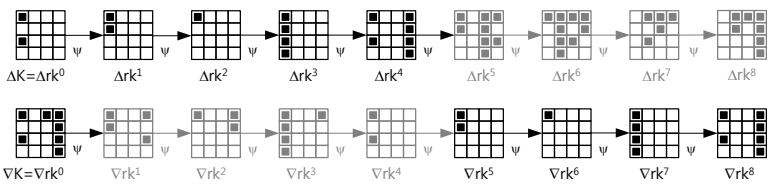

Fig. 8. Round key differential trails

6 Attack on Full Round SQUARE

6.1 Structure

We consider a fixed difference value ΔS defined by

$$\Delta S = (\mathtt{00}, \mathtt{00}, \mathtt{0a}, \mathtt{1e}, \quad \mathtt{00}, \mathtt{00}, \mathtt{00}, \mathtt{00}, \quad \mathtt{14}, \mathtt{0a}, \mathtt{0a}, \mathtt{1e}, \quad \mathtt{00}, \mathtt{00}, \mathtt{00}, \mathtt{00}).$$

In order to generate each structure $\mathcal{S}$, we choose arbitrary 8-bit constants $c_i \in \mathrm{GF}(2^8)$ for $i = 0, 1, \cdots, 13$, and define the following sets of plaintexts, $\mathcal{P}_1$ and $\mathcal{P}_2$

$$\mathcal{P}_1 = \{(\alpha, \beta, c_0, c_1, \cdots, c_{13}) | \alpha, \beta \in \mathrm{GF}(2^8)\},$$
$$\mathcal{P}_2 = \{P \oplus \Delta S | P \in \mathcal{P}_1\}.$$

The set $\mathcal{P}_1$ is a collection of 2^{16} plaintexts where all bytes are fixed except for the first two bytes. The set $\mathcal{P}_2$ is the collection of 2^{16} plaintexts generated by exclusive OR for each element in $\mathcal{P}_1$ with ΔS.

Note that the number of elements of both $\mathcal{P}_1$ and $\mathcal{P}_2$ are 2^{16}. We define a set $\mathcal{S}$ of 2^{33} ordered pairs as the following,

$$\mathcal{S} = \{(P_1, P_2) | P_1 \in \mathcal{P}_1, P_2 \in \mathcal{P}_2\} \cup \{(P_2, P_1) | P_1 \in \mathcal{P}_1, P_2 \in \mathcal{P}_2\}.$$

In $\mathcal{S}$, there are $2^{33-16} = 2^{17}$ pairs which satisfy the related-key differential trail for T as described in Figure 7, and we expect one right quartet per $2^{119-17} = 2^{102}$ structures. Let 2^m be the number of structures, then $m > 102$ for this attack.

6.2 Attack Procedure

Let us define the ciphertext difference ∇C by

$$\nabla C = (\mathtt{0a}, \mathtt{00}, \mathtt{0a}, \mathtt{00}, \quad \mathtt{00}, \mathtt{00}, \mathtt{00}, \mathtt{0a}, \quad \mathtt{0a}, \mathtt{00}, \mathtt{00}, \mathtt{00}, \quad \mathtt{00}, \mathtt{00}, \mathtt{00}, \mathtt{0a}).$$

The attack is done by the following steps for 2^m structures specified above.

1. Generate a structure $\mathcal{S}$ as described above.
2. For every element (P_1, P_2) in $\mathcal{S}$, do the following steps.
   (a) Calculate $C_1 = E_{K1}(P_1)$ and $C_2 = E_{K2}(P_2)$.

(b) Calculate $P_3 = E_{K3}^{-1}(C_1 \oplus \nabla C)$, $P_4 = E_{K4}^{-1}(C_2 \oplus \nabla C)$, and $\Delta Q = P_3 \oplus P_4$.
(c) If $\Delta Q \notin \mathcal{P}$ for $\mathcal{P}$ defined in (3), filter out out the quartet $((P_1, P_2), (P_3, P_4))$ (112-bit filter).
(d) If first two bytes difference of ΔQ can not be derived from `0x0a` and `0x0a` by inverse S-box operations, and exclusive OR with `0x14` and `0x0a` respectively, then filter out the quartet(2-bit filter).

3. If every quartet is filtered out, return to step 1.
4. For every candidate for the first two bytes of $\theta(K3)$, do the following steps.
   (a) Calculate each candidate for the first two bytes of $\theta(K1), \theta(K2)$, and $\theta(K4)$.
   (b) For every remained quartet, partially encrypt first two bytes of P_3 and P_4 with $\theta(K3)$ and $\theta(K4)$ for T. If the first two bytes of output difference of T are `0x0a` and `0x0a`, do the following step.
      – Partially encrypt first two bytes of P_1 and P_2 with $\theta(K1)$ and $\theta(K2)$ for T. If the first two bytes of output difference of T are `0x0a` and `0x0a`, then increase counter for the $\theta(K3)$.

After this procedures for 2^m structures, mostly counted 16-bit value is regarded as the first two bytes of $\theta(K3)$.

6.3 Attack Analysis

To prepare $m = 104$ structures for 4 right quartets, we need $2^{104+17} = 2^{121}$ plaintexts and 2 encryptions and 2 decryptions for each plaintexts, so the data complexity of this attack is 2^{123}. We expect that $2^{104+33-114} = 2^{23}$ quartets are left after filtering, and for each 2^{16} guessed partial keys, 4 times of 1/32 partial encryptions are needed for each quartet, so number of encryption for this attack does not exceed $2^{23+16+2-5} = 2^{36}$.

A pair (P_3, P_4) after filtering, proposes 4 candidates of 16-bit key information for first two bytes of both $\theta(K3)$ and $\theta(K4)$ and their related-key bytes are counted by pair (P_1, P_2) with probability 2^{-16}, so a quartet after filtering proposes one candidate of 16-bit key information with probability 2^{-14}. We have 2^{16} candidates for first two bytes of each $\theta(K1)$, $\theta(K2)$, $\theta(K3)$, and $\theta(K4)$, and 2^{23} pairs after filtering, thus every single candidate except for right key is proposed with probability $2^{23-14-16} = 2^{-7}$ compare to 4 for right key. Therefore, we regard this ratio as the signal to noise ratio as follows,

$$S/N = \frac{2^{m+33-119-16}}{2^{m-81-14-16}} = \frac{2^{m-102}}{2^{m-111}} = \frac{2^2}{2^{-7}} = 2^9 > 1.$$

After this attack, we have the first two bytes of $\theta(K1)$, $\theta(K2)$, $\theta(K3)$, and $\theta(K4)$. Other bytes of each key can be recovered exhaustive search for 2^{112} keys. Therefore, we can find a secret key of block cipher SQUARE faster than exhaustive search in related-key attack model.

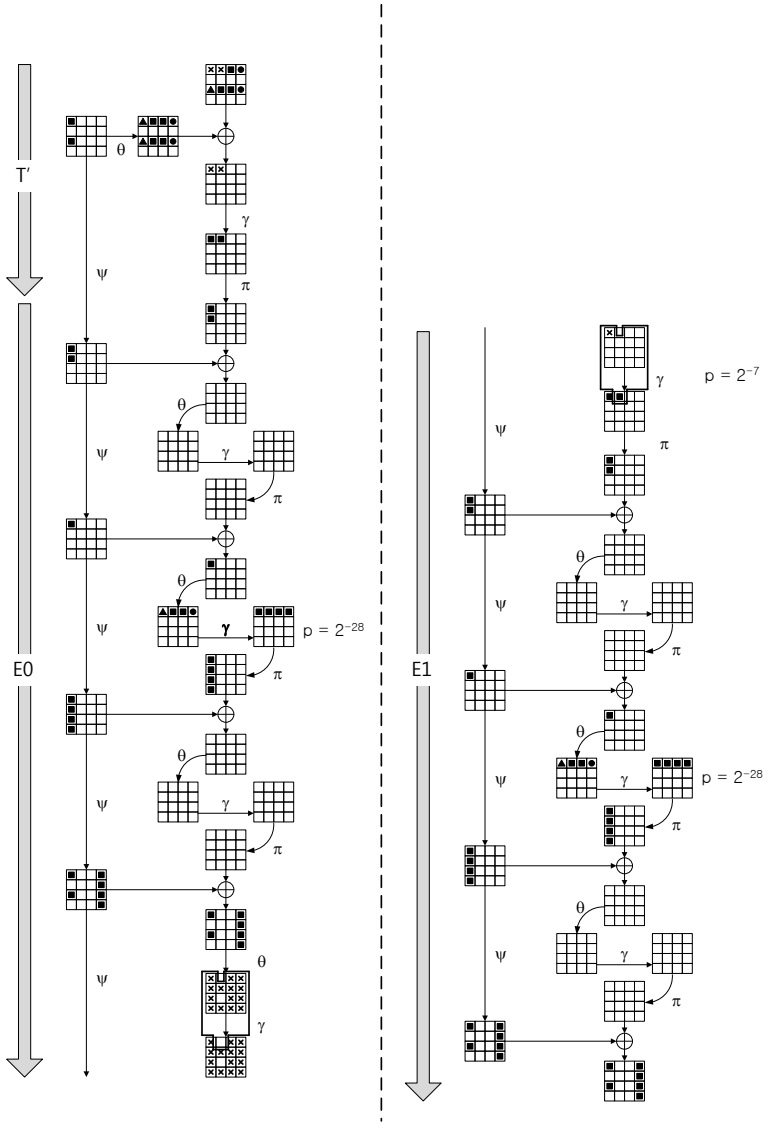

Fig. 9. A related-key boomerang attack of SQUARE

7 Conclusions

We present a related-key boomerang attack on the full round SQUARE. We find a 3-round related-key differential trail with high probability by local collision finding technique and construct 7-round boomerang distinguisher with them. Also, to estimate the distinguisher's probability more close to the real probability, we introduce local amplification technique and apply ladder switch. Even if this attack is not practical, considering similarity between SQUARE and AES-128 including key schedule, security of AES-128 against related-key attack model is still open.

References

1. Biham, E.: New types of cryptanalytic attacks using related keys. Journal of Cryptology, vol. 7(4): 229–246 (1994)
2. Biham, E., Dunkelman, O. Keller, N.: New results on boomerang and rectangle Attacks. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 507–525. Springer, Heidelberg (2005)
3. Biham, E., Dunkelman, O. Keller, N.: A related key Rectangle attack on full KASUMI. In: Roy, B.K. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 443–461. Springer, Heidelberg (2005)
4. Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D., Shamir, A.: Key Recovery Attacks of Practical Complexity on AES Variants With Up To 10 Rounds. Cryptology ePrint Archive, Report 2009/374
5. Biryukov, A., Khovratovich, D.: Related-key cryptanalysis of the full AES-192 and AES-256. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 1–18. Springer, Heidelberg (2009)
6. Biryukov, A., Khovratovich, D., Nikolić, I.: Distinguisher and related-key attack on the full AES-256. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5766, pp. 231–249. Springer, Heidelberg (2009)
7. Chabaud, F., Joux, A.: Differential collisions in SHA-0. In: Krawczyk, H. (ed.) CRYPTO '98. LNCS, vol. 1462, pp. 56. Springer, Heidelberg (1998)
8. Daeman, J., Knudsen, L.R., Rijmen, V.: The Block Cipher Square. In: Biham, E. (ed.) FSE '97. LNCS, vol. 1267, pp. 149–165. Springer, Heidelberg (1997)
9. Gorski, M., Lucks, S.: New Related-key Boomerang Attacks on AES. In: Chowdhury, D. R., Rijmen, V., and Das, A. (eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 266–278. Springer, Heidelberg (2008)
10. Kelsey, J., Kohno, T., Schneir, B.: Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent. In: Matsui, M. (ed.) FSE 2001. LNCS, vol. 1978, pp. 75–93. Springer, Heidelberg (2001)
11. U.S. National Institute of Standards and Technology.: Advanced Encryption Standard (AES), FIPS PUB 197. In: November 26, 2001, available at http://csrc.nist.gov/encryption/aes.
12. Wagner, D.: The boomerang attack. In: Knudsen, L.R. (ed.) FSE '99. LNCS, vol. 1636, pp. 156–170. Springer, Heidelberg (1999)